Вопросы и ответы

Мы очень серьезно относимся к своим обязательствам по защите конфиденциальной и частной информации наших клиентов и внедрились несколько усовершенствованных технологий для обеспечения безопасности информационных сетей, содержащих персональные данные наших клиентов.

Как многие другие государственные учреждения и организации, мы подвергаемся атакам со стороны хакеров (взломщиков), которые пытаются взломать наши компьютерные системы с целью кражи данных. К сожалению, недавно наша компьютерная система оказалась жертвой взлома, вследствие которого несанкционированные лица получили доступ к нашим серверам.

Что произошло?

С 19 апреля по 13 мая компьютерный вирус (W32.QAKBOT) заразил наши сети и рабочие места сотрудников Department of Unemployment Assistance (DUA, Отдел пособий по безработице штата Массачусетс), Department of Career Services (DCS, Отдел услуг по профессиональной ориентации) и некоторых центров комплексных услуг по профессиональной ориентации (One-Stop Career Centers). Узнав об этом, мы немедленно приняли меры, и с помощью компании Symantec, которая обеспечивает безопасность наших сетей, уничтожили вирус, поразивший наши сети и индивидуальные компьютеры.

Какие именно данные были скомпрометированы?

В результате заражения наших сетей компьютерным вирусом, существует вероятность утечки конфиденциальной информации о наших клиентах или сотрудниках. Эта информация может включать имя и фамилию, номер карточки социального обеспечения, адрес электронной почты, домашний или рабочий адреса. У нас есть основания предполагать, что только те клиенты, которые в указанный промежуток времени подавали в эти службы новые заявления или просили сотрудников этих служб помочь им в заполнении заявлений, и работодатели, которые подавали свои заявки в письменном виде, пострадали от утечки данных. Если Вы проверяли свои данные в онлайн-режиме, пользуясь DUA QUEST, WebCert или JobQuest,

и при этом не обращались за помощью к сотрудникам, то Ваши персональные данные не были скомпрометированы. В настоящее время наши сети полностью очищены от вируса, и компьютеры вне нашей сети не могут быть заражены при заполнении онлайн-заявлений.

Какие меры были приняты в связи с имевшей место утечкой данных?

Мы проводим внутреннее расследование с целью выявления причин нарушения безопасности сети, и мы пригласили специалистов по компьютерной безопасности, чтобы ввести новые дополнительные защитные механизмы и не допустить повторения утечки данных. Мы также работаем с официальными лицами на федеральном и штатном уровне для предотвращения подобных ситуаций в будущем и предпримем все необходимые действия, чтобы выявить и решить проблему.

Означает ли это, что я являюсь жертвой кражи личных данных?

Нет.

Тот факт, что кто-то мог получить доступ к Вашей информации не означает, что Вы являетесь жертвой кражи личных данных, или что получившие доступ лица намереваются использовать Вашу информацию с целью совершения мошеннических действий. Мы сочли нужным сообщить Вам об этом факте для того, чтобы Вы приняли меры для обеспечения защиты от возможных мошеннических действий.

Какие шаги следует предпринять, чтобы обезопасить себя?

Мы рекомендуем всем заявителям и клиентам центров комплексных услуг по профессиональной ориентации, а также бизнесам, которые подавали в эти центры заполненные вручную заявки, быть бдительными в отношении своей персональной информации и финансовых транзакций. Лицам, которые с 19 апреля по 13 мая пользовались услугами или были клиентами DCS, DUA, или One-Stop Career Center, и при этом во время доступа к своим данным в онлайн-режиме обращались за помощью к персоналу этих

учреждений, мы рекомендуем обратиться в кредитные агентства и попросить предупреждать их обо всех запросах, поступающих по их кредитным историям, в связи с возможной мошеннической деятельностью (fraud alert).

Вы имеете право на бесплатное получение своего кредитного отчета; Вы также имеете право на получение предупреждений о поступающих запросах на получение Вашего кредитного отчета (fraud alert) и на блокирование («замораживание») доступа к Вашей кредитной истории. Вы можете это сделать обратившись в одно из национальных агентств (бюро) по сбору и предоставлению информации о кредитоспособности потребителей (credit bureau). Как только одно из перечисленных ниже агентств получит Вашу просьбу о предупреждениях в случае поступления запросов о Вашей кредитной истории, она будет передана в два других агентства (бюро). Как правило, просьба о предупреждениях действительна в течение 90 дней, но это срок может быть продлен. За эту услугу (предупреждения о возможной мошеннической деятельности) плата не взимается. Однако имейте в виду, что агентства могут взимать плату (5 долларов) за то, чтобы заморозить доступ к Вашей кредитной истории, разрешить временный доступ, или полностью восстановить доступ (снять «замораживание») к Вашей кредитной истории. Каждое из трех кредитных агентств бесплатно предоставляет потребителям их кредитные отчеты один раз в 12 месяцев. Ниже приводятся данные трех кредитных бюро:

«Эквифакс» (Equifax): (800) 525-6285 (<http://www.equifax.com>)

«Экспириан» (Experian): (888) 397-3742 (<http://www.experian.com>)

«ТрансЮнион» (TransUnion): (800) 680-7289 (<http://www.tuc.com>)

Вы также можете получить дополнительную информацию о краже личных данных и о том, как обезопасить свою персональную информацию на нашем веб-сайте по адресу <http://1.usa.gov/jcLaDY>, или позвонить в Исполнительный офис департамента труда и подготовки трудовых ресурсов по телефону **1-877-232-6200**.

Могут ли мне позвонить из государственных органов штата и задать вопросы о моих персональных данных в связи с этим событием?

Мы никогда не просим клиентов предоставлять нам такую персональную информацию, как номер карточки социального

обеспечения (Social Security number), кредитной карточки или информацию о банковских счетах. Если Вам позвонят по телефону или отправят Вам на адрес электронной почты просьбу предоставить персональную информацию, мы просим Вас сообщить о таких звонках и электронных сообщениях в местное отделение полиции, офис прокурора округа (District Attorney's Office), или офис Генерального прокурора (Attorney General's Office).

Что делать, если у меня есть основания считать, что я являюсь жертвой кражи персональных (личных) данных?

Если Вы считаете, что стали жертвой кражи личных данных, Вы должны сообщить об этом преступлении в подразделение борьбы с мошенничеством (fraud division) Вашего местного отделения полиции. Кроме того, если Вы полагаете, что Ваша персональная информация может быть использована для поступления на работу, Вы должны сообщить об этом в Internal Revenue Service (IRS, Федеральная налоговая служба) и Social Security Administration (SSA, Управление социального обеспечения).